Netzwerk Datenschutzexpertise GbR
Dr. Thilo Weichert
Waisenhofstr. 41
D-24103 Kiel
Tel.: +49 431 9719742
E-Mail: weichert@netzwerk-datenschutzexpertise.de

DR. THILO WEICHERT, WAISENHOFSTR. 41, 24103 KIEL

An den Deutschen Bundestag
Ausschuss für Inneres und Heimat
Platz der Republik 1, 11011Berlin

Kiel, den 24.04.2021

Stellungnahme des Netzwerks Datenschutzexpertise

zum Gesetzentwurf der Bundesregierung
Entwurf eines Gesetzes zur Weiterentwicklung des Ausländerzentralregisters (AZRWeiterentwG)
BT-Drs. 19/28170 v. 2.03.2021 (entspricht BR-Drs. 186/21 v. 25.02.2021
Bezug: Ihre Mail vom 23.04.2021, Leiter Sekretariat PA 4

Sehr geehrte Frau Vorsitzende Andrea Lindholz,
sehr geehrte Damen und Herren Abgeordnete,

vielen Dank für Ihre Einladung zur öffentlichen Anhörung am 03.05.2019 zu dem im Betreff genannten Gesetz, an der ich gerne teilnehmen werde.

A Zum Gesetzentwurf generell

Der Entwurf zielt auf eine verstärkte informationelle Verzahnung von an das Ausländerzentralregister (AZR) angebundenen Behörden durch eine Änderung des Ausländerzentralregistergesetzes (AZRG) und durch weitere ausländerrechtliche Regelungen zur Datenverarbeitung. Das AZRG ist seit seinem erstmaligen Inkrafttreten im Jahr 1994 über 40 Mal geändert worden. Abgesehen davon, dass das Gesetz nach einem Urteil des Europäischen Gerichtshofs (EuGH) vom 16.12.2008[1] mit Gesetz vom 20.12.2012 im Hinblick auf die Verarbeitung von Daten von EU-Ausländern eingeschränkt werden musste, zielten alle weiteren Änderungen des AZRG darauf ab, die Verarbeitungsbefugnisse der Behörden zu erweitern, ohne zugleich die Garantien für den Datenschutz der Betroffenen zu verbessern. Dies hat dazu geführt, dass das AZRG immer stärker in das Recht auf informationelle Selbstbestimmung bzw. in das Grundrecht auf Datenschutz der betroffenen Ausländerinnen und Ausländer sowie in weitere Grundrechte eingreift. Der Grundrechtszustand hat sich immer weiter verschlechtert mit der Folge, dass das derzeit geltende Gesetz – unabhängig von den aktuell geplanten Änderungen – **gegen verfassungs- und europarechtliche Vorgaben verstößt**, etwa gegen das datenschutzrechtliche Zweckbindungsgebot, den Erforderlichkeitsgrundsatz und das Prinzip der Datenminimierung, die Transparenzpflicht gegenüber den Betroffenen sowie den Gleichbehandlungsgrundsatz bzw. das Diskriminierungsverbot. Diese verfassungs- und europarechtlichen Defizite können in der vorliegenden Stellungnahme nicht detailliert dargestellt werden. Der vorliegende Entwurf verstärkt die informationellen Eingriffe und damit die bisherigen Defizite.

[1] EuGH U.v. 16.12.2008 – C-524/06, NVwZ 2009, 379 = MMR 2009, 171 = DVBl 2009, 171 = ZAR 2009, 197.

Mit dem Gesetzentwurf soll eine grundlegende Veränderung der Datenverarbeitung im Ausländerwesen eingeleitet werden. Ziel ist es mittelfristig, die bisherigen dezentralen Datenbestände in Ausländerbehörden (Ausländerdatei A) durch die **zentrale Datenführung ausschließlich im AZR** zu ersetzen, um Datenredundanzen zu vermeiden, den Datenaustausch zwischen verschiedenen Behörden zu erleichtern und durch Synchronisation die Aktualität und Richtigkeit der gespeicherten Daten zu verbessern.

Diese Planung erfolgt parallel zum generellen Versuch, die Modernisierung der digitalen Datenverarbeitung in der Verwaltung zu erreichen, die mit dem jüngst beschlossenen Registermodernisierungsgesetz (RegMoG) vorangetrieben wird, mit dem eine bundesweit gültige Identifikationsnummer (ID-Nummer), die für jede Person zweckübergreifend verwendet wird, eingeführt werden soll.[2] Durch dieses RegMoG wird zusätzlich zur AZR-Nummer mit der ID-Nummer eine redundantes nationales Kennzeichen im Ausländerbereich eingeführt (vgl. Art. 87 DSGVO). Eine Redundanz entsteht nun auch mit einer parallelen Datenhaltung im AZR und bei den Ausländerbehörden. Diese doppelte Datenhaltung verstößt gegen den europaweit verbindlichen Grundsatz der Datenminimierung (Art. 5 Abs. 1 lit. c DSGVO). Ein solcher Verstoß kann allenfalls vorübergehend hingenommen werden, bis die Umstellung der Datenhaltung abgeschlossen ist. Das **Verbot einer redundanten Datenhaltung** gilt sowohl für nationale Kennnummern (AZR-Nummer, ID-Nummer) wie auch generell für die Datenhaltung im Ausländerrecht (AZR, Ausländerdatei A).

Der Entwurf zielt darauf ab, die **Datenqualität im Bereich des Ausländerrechts** zu erhöhen, indem alle Behörden, die mit der Durchführung von ausländer- und asylrechtlichen Vorschriften betraut sind, auf denselben einheitlichen und aktuellen Datenbestand zugreifen können. Dadurch soll sowohl die Bearbeitungsgeschwindigkeit wie auch die Qualität von aufenthalts- und asylrechtlichen Verfahren erhöht werden. Eine solche Intention ist grundsätzlich zu begrüßen. Derartige Änderungen müssen aber, um nicht nur den Verwaltungsinteressen, sondern auch den Belangen der Betroffenen zu entsprechen, mit einer Einbindung der Betroffenen und einer Verbesserung der Transparenz für diese einhergehen. Leider enthält der Gesetzesvorschlag hierzu bisher keine Regelungen.

Der zugrunde liegende Referentenentwurf nahm für sich in Anspruch, das **once-only-Prinzip** im Ausländerwesen zu verwirklichen. Das once-only-Prinzip wird damit beschrieben, dass Daten im Bereich der öffentlichen Verwaltung nur einmal erhoben werden müssen. Zentrale und dezentrale Datenbestände sollen untereinander synchronisiert werden. Es werde eine zentrale Dokumentenablage im AZR für die Ausländer- und Asylbehörden und für weitere Stellen geschaffen. Damit wird aber nur eine Seite des once-only-Grundsatzes beschrieben. Der Grundsatz soll zugleich auch eine Verringerung des Aufwands für die Betroffenen und eine Verbesserung der Bürgerfreundlichkeit der Verwaltung mit sich bringen.[3] Der vorliegende Gesetzesentwurf sieht insofern keine Verbesserungen vor. Vielmehr steht zu befürchten, dass der Austausch der Daten über die Betroffenen hinter deren Rücken dazu führt, dass Fehler vertieft und die Partizipation der Betroffenen verschlechtert werden. Dies mag der Grund sein, dass im vorliegenden Gesetzentwurf nicht mehr ausdrücklich auf das once-only-Prinzip verwiesen wird.

Mit der Zentralisierung der Datenhaltung im AZR erfolgt ein grundlegender Wechsel, der zu weiteren gesetzlichen Änderungen führen muss. Bei einer derartigen grundlegenden Weichenstellung ist es geboten, die Gesamtstruktur der ausländerrechtlichen Datenverarbeitung zu hinterfragen. Der Europäische Gerichtshof hat festgestellt, dass aus Gründen des Grundrechtsschutzes eine dezentrale Datenhaltung einer zentralen

[2] G. v. 28.03.2021, BGBl. I S. 591.
[3] Big Data Value Association, Towards a European Data Sharing Space, April 2019, S. 6; European Commission, EU-wide digital Once-Only Principle for citizens and businesses – Policy options and their impacts, 01.02.2017.

Datenhaltung vorzuziehen ist, wenn auch so die verfolgten Zwecke erreicht werden können.[4] Aus diesem Grund bedarf es vor einer umfassenden Neustrukturierung der Feststellung der Notwendigkeit von Folgeänderungen. Angesichts der verstärkten Integration innerhalb der Europäischen Union und der Angleichung der Rechte von EU-Staatsangehörigen an die Rechte von deutschen Staatsangehörigen sollte eine **Dezentralisierung der Datenhaltung über EU-Staatsangehörige** ausschließlich bei den Ausländerbehörden geprüft werden. Dies würde zugleich zu einer Bereinigung und einer Vereinfachung des AZR-Datenbestands führen.

B Zu den einzelnen Regelungsvorschlägen

Sämtliche Stellungnahmen zum Gesetzentwurf beziehen sich auf den Art. 1 (im Klammer die jeweilige Ziffer) zur Änderung des AZRG.

Zu § 3 Abs. 1 AZRG (3.) – zusätzliche Merkmale

Es ist vorgesehen, den allgemeinen Datensatz von allen im AZR gespeicherten Personen auszuweiten um folgende **weitere Merkmale**: Geburtsland, Doktorgrad, ausländische Personenidentitätsnummer, Anschrift im Bundesgebiet und Einzugsdatum, frühere Anschriften im Bundesgebiet und Auszugsdatum, nationale Visumsverlängerung, Angaben zu Arbeits- und Ausbildungsvermittlung und zu Integrationskursen.

Die zusätzliche Speicherung des **Doktorgrads** (Nr. 4) im AZR wird ausschließlich damit begründet, dass dieses Datum bisher in der Ausländerdatei A der Ausländerbehörden gespeichert sei und dieser Datenbestand nun zentralisiert werde (Entwurf S. 72). Auch wenn das Merkmal keine hohe Sensitivität hat, so ist es ein personenbezogenes Datum mit einer gewissen Aussagekraft. Dessen Erforderlichkeit für eine bundesweit zentralisierte Speicherung ist ebenso wenig wie für eine dezentrale Speicherung nicht erkennbar.

Die **ausländische Personenidentitätsnummer** (CNP-Nummer - Code Numeric Personal) nach Nr. 5b soll eine eindeutige Identifizierung auch bei Namensänderung gewährleisten (Entwurf S. 72). Sie ermöglicht zugleich aber auch die Erschließung von vielfältigen Datenbeständen in einem Herkunftsland. Über diese Nummer können deutsche Daten mit solchen des Herkunftslandes einfach zusammengeführt werden. Diese Möglichkeit soll insbesondere künftig auch Sicherheitsbehörden eröffnet werden (§ 6 Abs. 1 Nr. 2, 4 ff. AZRG, § 6 Abs. 2 S. 3 Nr. 1, 2, 44, 4a, 5, 5a AZRG-E). Genutzt werden können soll die Nummer im Rahmen von Ersuchen nach § 5 AZRG – für alle öffentlichen Stellen (§ 6 Abs. 4 AZRG-E) sowie insbesondere ohne Einschränkungen für Sicherheitsbehörden (§§ 15, 20 AZRG). Die ausländische Personenidentitätsnummer soll künftig auch als eindeutiger Identifikator für Übermittlungen von Zoll- und Sozialbehörden genutzt werden können (z.B. § 17 Abs. 1 Nr. 5a AZRG-E sowie im Entwurf die Nrn. 14-20).

Bei diesen CNP-Nummern handelt es sich um **nationale Kennzeichen** i.S.v. Art. 87 Datenschutz-Grundverordnung (DSGVO). Dadurch wird das Risiko massiv erhöht, dass Daten aus dem Ausland am Betroffenen vorbei erhoben oder dorthin übermittelt werden. Gemäß Art. 87 S. 2 DSGVO ist die Verwendung solcher Nummern nur „unter Wahrung geeigneter Garantien für die Rechte und Freiheiten der betroffenen Person“ zulässig. Derartige spezifische Schutzvorkehrungen sieht der Entwurf nicht vor. Die Behauptung der BReg, eine Übermittlung der CNP-Nummer an ausländische Behörden sei durch die § 26 AZRG „gesetzlich ausgeschlossen“[5] findet in der benannten Regelung keine Grundlage. Ebenso wenig ausgeschlossen ist eine Übermittlung der CNP-Nummer insbesondere durch deutsche Sicherheitsbehörden, die diese Nummer vom AZR erhalten und weiterverarbeiten

[4] EuGH U. v. 16.12.2008 – C-524/06 (Fn. 1), Rn. 62.
[5] Antwort Nr. 7 u. 8 der BReg v. 13.04.2021 auf die kleine Anfrage BT-Drs. 19/28123.

dürfen (§§ 15, 20 AZRG) und potenziell an Behörden in Drittstaaten übermitteln. Daher sind die geplante Regelung und die Folgeregelungen hierzu europarechtswidrig.

Die Speicherung von **deutschen Wohnadressen** (Nrn. 5c, 5d) galt bisher nur für Flüchtlinge und wird nun auf sämtliche Nicht-EU-Bürger erweitert. Die Wohnadressen werden bisher dezentral für die Verwaltung in den kommunalen Meldebehörden vorgehalten und zur Verfügung gestellt. Die Speicherung im AZR soll zusätzlich erfolgen. Begründet wurde dies im Referentenentwurf mit der effizienteren Gestaltung des Verfahrensablaufs, nun mit dem formalen Verweis darauf, dass diese Daten auch bei den Ausländerbehörden verfügbar sind (Entwurf S. 76). Die Speicherung hat zur Folge, dass diese Daten einfacher und trotz ihres möglicherweise bestehenden hohen Schutzbedarfs ohne die nach dem Melderecht geltenden Schutzvorkehrungen (§§ 51, 53 BMG) verfügbar gemacht werden. Die Erforderlichkeit ist nicht hinreichend begründet. Ohne entsprechende Schutzvorkehrungen ist diese Zusatzspeicherung in jedem Fall unverhältnismäßig. Zudem stellt diese Regelung eine unzulässige Diskriminierung von Nicht-EU-Bürgern gegenüber EU-Bürgern wegen der Staatsangehörigkeit dar (Art. 21 Abs. 2 GRCh).

Die Erforderlichkeit der ausnahmslosen zentralen Speicherung von **Vermittlungs- und Integrationsmaßnahmen** (Nr. 9) und der dadurch bedingten Verfügbarmachung für Dritte ist im Entwurf nicht begründet und auch nicht erkennbar. Es handelt sich um sensible Informationen, die Rückschlüsse auf prekäre Lebenssituationen erlaufen (Arbeits- und Integrationsprobleme). Vorkehrungen zur Sicherung der Zweckbindung und zur Wahrung der Schutzinteressen der Betroffenen sind nicht geregelt.

Zu § 5 Abs. 5 AZRG (4.) – Verlängerung der Suchvermerk-Speicherfrist

Die Regelung sieht vor, dass Suchvermerke sowie die hierzu übermittelten Daten, die bisher längsten zwei Jahre lang gespeichert werden, in Zukunft bis zu drei Jahr lang gespeichert werden dürfen. Im Referentenentwurf war sogar eine Verlängerung der Speicherfrist auf sechs Jahre geplant. Die Ausweitung wurde im Referentenentwurf damit begründet, dass es insbesondere darum gehe, Ausländer mit **unbekanntem Aufenthaltsort aufzuspüren**, wenn diese sich Kostenerstattungspflichten entziehen. Die Dauer wurde mit der Fälligkeitsverjährung der Ansprüche auf Erstattung von Kosten gerechtfertigt. Die nun vorgeschlagene Dreijahresfrist wird begründet mit der Parallelität zu § 29 BZRG, ohne dass darauf eingegangen wird, dass die Fahndungsausschreibung im Bundeszentralregister nur unter engeren Voraussetzungen erlaubt wird und eine weitgehende andere Zielsetzung verfolgt als § 5 AZRG.

Die Regelung erstreckt sich auf jede Form behördlicher Aufenthaltsermittlung. Dies kann eine polizeiliche oder geheimdienstliche Ermittlung sein, ebenso wie ein Ersuchen zur Durchsetzung der Schulpflicht. Die Regelung ist schon bisher wegen ihrer **Unbestimmtheit** verfassungswidrig, da sie keinen Zweck der Suche benennt und keine Erheblichkeitsschwelle oder Verfahrensanforderung (z.B. Richtervorbehalt) und keine Abwägung im Einzelfall vorsieht.[6]

Die Regelung ist **nicht erforderlich**. Bisher ist es möglich, nach 2 Jahren eine erneute Speicherung für 2 Jahre eintragen zu lassen. Die bisherige Zweijahresfrist gewährleistet wenigstens, dass nach 2 Jahren eine Einzelfallprüfung erfolgen muss. Die neue Regelung hätte zur Folge, dass der Suchvermerk für einen Betroffenen 3 Jahre lang gespeichert sein kann, ohne dass er hiervon Kenntnis erlangen muss, was wegen der umfangreichen Verfügbarkeit der Suchinformationen in praktisch allen öffentlichen Stellen mit einem verstärkten Diskriminierungsrisiko verbunden ist.

[6] Weichert, AZRG, 1998, § 5 Rn. 5, 8.

Zu § 6 Abs. 5 (5. lit. f)

Bisher war schon vorgesehen, dass über das AZR **Begründungstexte** verfügbar gemacht werden. Schon die aktuelle Regelung steht unter starker rechtlicher Kritik, weil die verfügbar gemachten Begründungstexte aus ihrem Aktenkontext herausgezogen werden und die Begründungstexte für einen weiteren Zweck verwendet werden, ohne dass den Betroffenen Kenntnis und die Möglichkeit zur Stellungnahme gegeben wird. Zudem war nicht sichergestellt, dass ausschließlich rechtsbeständige Begründungstexte verfügbar gemacht werden, so dass Entscheidungen weiterübermittelt werden, die möglicherweise inzwischen aufgehoben worden sind.[7]

Die Änderung sieht nun vor, dass erheblich **mehr Dokumente** gespeichert werden und dass diese digital übermittelt werden können: Entscheidungen des Bundesamts für Migration und Flüchtlinge (BAMF), der Ausländerbehörden und von Gerichten zum Aufenthaltsrecht, die Beschränkung/Untersagung der politischen Betätigung, der Verlust der Freizügigkeit für EU-Bürger, Entscheidungen über Einreisebedenken sowie ausländische Ausweis- oder Identifikationsdokumente an das AZR. Bei asylrechtlichen Entscheidungen muss geprüft werden, ob „besondere gesetzliche Verarbeitungsregelungen oder überwiegende schutzwürdige Interessen des Ausländers“ entgegenstehen.

Die Regelung stellt, mehr als bisher, sicher, dass die verfügbaren Dokumente vollzählig/vollständig sind, so dass ein geringeres Risiko besteht, dass nicht mehr aktuelle oder gar inzwischen aufgehobene Entscheidungen bei den abrufenden Stellen zur Grundlage von Entscheidungen genommen werden. Dieses Risiko besteht aber weiterhin, zumal es keine Überprüfungspflicht bzgl. der **Vollständigkeit und Aktualität der Dokumente** vor einer Übermittlung gibt und die Betroffenen über diese Übermittlung und deren Inhalt nicht informiert werden.

Hinsichtlich der Übermittlung von Asylentscheidungen ist die Übermittlung der Dokumente zwangsläufig mit der Übermittlung von Angaben verbunden, die der Betroffene zu seiner **politischen oder sonstigen Verfolgung** und zu sonstigen äußerst sensiblen Sachverhalten gemacht hat. Die Regelung, dass schutzwürdige Betroffeneninteressen zu berücksichtigen sind, ist prozedural nicht abgesichert und unterliegt einem weiten Beurteilungsspielraum des AZR, ohne dass bisher eine Anhörung oder Einbindung der Betroffenen vorgesehen, geschweige denn sichergestellt wäre. Die zentrale Verfügungsmöglichkeit der Daten kann zu einem massiven Schaden und zu einer starken Verunsicherung für die Betroffenen führen.[8]

Die Entwurfsverfasser scheinen die Sensitivität von im AZR gespeicherten Daten nur begrenzt erfasst zu haben, da sie zwar wortreich begründen, weshalb in Asylbescheiden Gesundheitsdaten enthalten sein dürfen, die nach Art. 9 Abs. 1 DSGVO besonders geschützt sind. Dass **Art. 9 Abs. 1 DSGVO** Daten, aus denen „politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen“, spezifisch geschützt werden müssen, wird nicht erwähnt (S. 78 f.). Gerade solche Meinungen, Überzeugungen und Zugehörigkeiten finden sich insbesondere in Asylbescheiden und begründen oft eine Verfolgungsgefahr im Herkunftsland. Die Verarbeitung von Daten nach Art. 9 Abs. 1 DSGVO ist im konkreten Fall „aus Gründen eines erheblichen öffentlichen Interesses“ nur erlaubt, wenn „angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person“ sichergestellt sind (Art. 9 Abs. 2 lit. g DSGVO). Das erhebliche öffentliche Interesse ist nicht hinreichend dargetan; das Fehlen von spezifischen Schutzmaßnahmen macht die Regelung europarechtswidrig.

[7] Weichert, AZRG, 1998, Art. 6 Rn. 23-26.
[8] Siehe hierzu den anschaulichen Fall eines BA-Mitarbeiters, der Informationen aus dem AZR nutzte, um einen ägyptischen Flüchtling über das Internet einzuschüchtern, DANA 3/2019, 155 f.

Zu § 8a (6.):

Es ist geplant, im AZRG einen § 8a einzuführen, der einen Abgleich zwischen dem AZR (Registerbehörde) sowie der aktenführenden bzw. Daten anliefernden Stelle legitimiert bei berechtigten Zweifeln an der **Richtigkeit und Aktualität der Daten**. Die Zielrichtung der Regelung unterstützt die beteiligten Stellen bei der Umsetzung des Grundsatzes der Datenrichtigkeit (Art. 5 Abs. 1 lit. d DSGVO).

Zumindest problematisch ist aber der **große Kreis an Stellen**, mit denen das AZR einen Datenabgleich durchführen kann. Angesichts des Umstands, dass die Zahl und Qualität der Daten anliefernden Stellen fast unbegrenzt ist (§§ 5, 6 AZRG), besteht auch mit all diesen Stellen die Befugnis zu einem Datenabgleich. § 8a Abs. 2 des Entwurfs enthält eine eigenständige wechselseitige Übermittlungsbefugnis, bei der die im AZRG noch enthaltenen rudimentären Zweckbindungsregelungen bzw. Datenkranzbeschreibungen nicht explizit gelten. Die einzige materielle oder formelle Hürde besteht darin, dass „Zweifel an der Richtigkeit und Aktualität der Daten" bestehen. Dies erweitert das Risiko, dass Daten ausgetauscht werden, die zweckwidrig weitergenutzt werden können.

Zu § 10 (7.)

Gemäß § 10 Abs. 2 S. 2 genügt für die Identifizierung eines Betroffenen für eine Datenübermittlung an eine andere Stelle neben dem Lichtbild oder den Fingerabdruckdaten künftig die Anfrage über die dazugehörigen **Referenznummern**. Schon die bisherige Regelung ist problematisch, da mit Hilfe der **biometrischen Daten** eine Fahndung im AZR-Datenbestand ausgelöst werden kann.[9] Eine Erforderlichkeit der bisherigen Regelung, die nach Regierungsangaben bisher nicht genutzt wird[10], ist nicht dargetan. Angesichts der Fehleranfälligkeit biometrischer Zuordnungen besteht das Risiko, dass über solche Anfragen sensible Daten dritter Personen übermittelt werden. Diese Gefahr kann durch eine zusätzliche Angabe der Referenznummer reduziert werden. Verstärkt fehleranfällig ist dagegen, dass mit der geplanten Regelung es auch erlaubt wird, ausschließlich über die Referenznummer Übermittlungsersuchen vorzunehmen.

Zu § 22 Abs. 1 S. 1 Nr. 5a (23.; BT-Drs. 19/28170 Art. 1 Nr. 21)

Bisher waren Gerichte der **Sozialgerichtsbarkeit und der Verwaltungsgerichtsbarkeit** nur befugt, Grunddaten eines Ausländers automatisiert aus dem AZR abzurufen. In Zukunft soll diese Beschränkung wegfallen, so dass diese Gerichte sämtliche als relevant angesehenen Daten online abfragen können. Damit soll eine ungerechtfertigte Ungleichbehandlung gegenüber den zugriffsberechtigten Behörden beseitigt werden. Angaben zum aufenthaltsrechtlichen Status sowie zu ergriffenen Maßnahmen seien für die Gerichte nötig, etwa bei Verfahren des einstweiligen Rechtsschutzes (Entwurf S. 86). Die Begründung genügt nicht für eine Erläuterung der Erforderlichkeit: Verfahrensbeteiligt sind in jedem Fall Behörden, die einen umfassenden AZR-Onlinezugriff haben. Es ist zumutbar, dass diese Behörden ihrer Pflicht nachkommen, die für die Gerichtsverfahren relevanten Informationen dem Gericht zur Verfügung zu stellen.

[9] Weichert, Staatliche Identifizierung mit Fingerabdrücken und biometrischen Lichtbildern, 08.03.2021, Kap. 5.1, https://www.netzwerk-datenschutzexpertise.de/sites/default/files/gut_2021biometrischeidentifizierung.pdf.
[10] Antwort Nr. 4 u. 5 der BReg v. 13.04.2021 auf die kleine Anfrage BT-Drs. 19/28123

C Änderungsvorschläge

Mit den folgenden Änderungsvorschlägen kann die europa- und verfassungsrechtliche Problematik des AZRG nicht behoben werden, wohl aber in Bezug auf den vorliegenden Gesetzesentwurf gelindert werden.

1. § 5 AZRG zu **Suchvermerken** wird insgesamt gestrichen. Hilfsweise wird auf die Verlängerung der Geltungsdauer von zwei auf drei Jahre verzichtet.

Begründung
§ 5 ist insgesamt verfassungswidrig. Eine Verlängerung der Geltungsdauer von Suchvermerken ist nicht erforderlich (s.o. B 4.).

2. In § 10 wird ein neuer Absatz 1b eingefügt mit folgendem Wortlaut:

„Die in § 3 Absatz 1 Nummer 9, Absatz 2 Nummern 10, 10a und 11 aufgeführten Daten dürfen nur unter den Voraussetzungen übermittelt werden, unter denen Sozialleistungsträger Sozialdaten übermitteln dürften. Die §§ 67e bis 75 SGB X sind entsprechend anwendbar."

Begründung
Die in dem Regelungsvorschlag aufgeführten Daten stammen von Sozial- und Gesundheitsbehörden oder weisen eine entsprechende Sensitivität auf. Insofern besteht auch bei einer Übermittlung durch das AZR ein dem Sozialgeheimnis (§ 35 SGB I) entsprechender Bedarf an Wahrung der Vertraulichkeit. Dem wird dadurch Rechnung getragen, dass die Übermittlungsregelungen für Sozialdaten für das AZR entsprechend anwendbar sind.

3. In § 10 Abs. 2 S. 2 wird das Wort „nur" gestrichen.

Begründung
Der bisherige Wortlaut erlaubt eine Fahndung im AZR allein mit Lichtbild oder Fingerabdruck. Von diesem Recht wird bisher gemäß der Auskunft der Bundesregierung kein Gebrauch gemacht (s.o. B 7.). Eine derartige **Nutzung der biometrischen Daten** wäre unverhältnismäßig und verfassungswidrig und ist auszuschließen.

4. Bei dem geplanten § 10 Abs. 6 wird folgender Satz 2 angefügt:

„Der Ausländer wird über die Übermittlung unverzüglich informiert."

Begründung
Die Regelung ist eine Umsetzung von Art. 14 DSGVO, der vorsieht, dass Betroffene über Übermittlungen informiert werden, wenn die Daten beim Empfänger nicht direkt erhoben werden (s.o. B 5. lit. f). Die Information erhöht die Transparenz und ermöglicht dem Betroffenen, seinen Standpunkt darzustellen und evtl. Rechtsschutz in Anspruch zu nehmen.

5. In § 11 (Zweckbestimmung, Weiterübermittlung von Daten) wird ein neuer Absatz 1b mit folgendem Wortlaut eingefügt:

„Übermittlungsempfänger dürfen die ausländische Personenidentitätsnummer (§ 3 Abs. 1 Nr. 5b) nicht an ausländische Stellen weiterübermitteln."

Begründung
Mit der Einführung der **ausländischen Personenidentitätsnummer** in den AZR-Datenbestand wird die Gefahr begründet, dass diese auch im Ausland und insbesondere

durch Behörden des Heimatstaats verwendet werden (s.o. B 3.). Durch die Ergänzung soll dies ausgeschlossen werden.

6. Es wird folgender § 34a eingefügt:

§ 34a **Datencockpit**

(1) Das AZR betreibt ein Datencockpit, mit dem sich eine betroffene Personen Datenübermittlungen durch das AZR, bei denen eine AZR-Nummer nach § 3 Abs. 1 Nr. 2 zum Einsatz kommt, anzeigen lassen kann.
(2) Im Datencockpit werden zu jeder Übermittlung der Empfänger, das Datum sowie der Übermittlungsinhalt angezeigt. Diese Daten werden im Datencockpit nur für die Dauer des jeweiligen Nutzungsvorgangs gespeichert; nach Beendigung des Nutzungsvorgangs sind sie unverzüglich zu löschen.
(3) Jede betroffene Person kann sich beim Bundesamt für Migration und Flüchtlinge für das Datencockpit registrieren. Sie hat sich unter Angabe ihrer Grundpersonalien auf dem Vertrauensniveau hoch zu identifizieren. § 10 Abs. 3 S. 3 und 4 Onlinezugangsgesetz findet entsprechend Anwendung.
(4) Der Nutzer legt fest, in welchem Umfang ihm Datenübermittlungen angezeigt werden. Auf diese Daten hat nur der Nutzer Zugriff. Der Nutzer muss sein Konto im Datencockpit jederzeit selbst löschen können. Das Konto im Datencockpit wird automatisch gelöscht, wenn es drei Jahre nicht verwendet wurde.

Der bisherige § 34a wird zu § 34b.

Begründung
Die Regelung entspricht § 10 Onlinezugangsgesetz (OZG)[11], der als Kompensationsmaßnahme für die Nutzung einer nationalen Kennziffer, der ID-Nummer, eine verbesserte Transparenz herstellt. Es handelt sich um eine Garantiemaßnahme i.S.v. Art. 87 DSGVO, da es sich bei der AZR-Nummer ebenso wie bei der ID-Nummer um ein „Kennzeichen von allgemeiner Bedeutung“ handelt (s.o. unter A). Die Regelung ermöglicht es der Bundesverwaltung, das im OZG geplante Datencockpit in einem einfacheren rechtlichen und technischen Rahmen zu erproben.

7. In **§ 51 Bundesmeldegesetz** (BMG) wird ein Absatz 6 eingefügt mit folgendem Wortlaut:

„Im Fall einer Auskunftssperre zugunsten eines Ausländers wird das Ausländerzentralregister umgehend informiert.“

Begründung
Zwar sieht § 4 Abs. 2 S. 2 AZRG vor, dass § 51 Abs. 1 und 5 BMG im AZR entsprechend gelten, der eine Auskunftssperre aus Gründen des Personenstandsrechts sowie bei einer „Gefahr für Leben, Gesundheit, persönliche Freiheit oder ähnliche schutzwürdige Interessen“ vorsieht. Es ist aber nicht gewährleistet, dass das AZR von einer melderechtlichen Auskunftssperre erfährt, so dass eine Übermittlungssperre i.S.v. § 4 AZRG eingerichtet werden kann. Die Übermittlung ist erforderlich, um gefährdete Ausländer vor für sie schädlichen Datenübermittlungen zu bewahren.

D Fazit

Der Gesetzentwurf reiht sich ein in vorangegangene Änderungen des AZRG, mit denen ein europarechts- und verfassungsrechtswidriger Zustand vertieft wird. Gegen eine Modernisierung der digitalen Kommunikation im Ausländerwesen ist nichts einzuwenden.

[11] I.d.F. v. G. v. 28.03.2021, BGBl. I S. 591.

Doch muss diese, um nachhaltig sein zu können und den legitimen Betroffeneninteressen zu entsprechen, den nationalen und europäischen grundrechtlichen Anforderungen genügen. Das BVerfG nahm mit Beschluss vom 10.10.2001 eine Verfassungsbeschwerde gegen das AZRG nicht an, stellte aber fest, dass die Beschwerde „durchaus gewichtige verfassungsrechtliche Fragen“ aufwirft. Über die Beschwerde konnte aber wegen des fehlenden Nachweises einer unmittelbaren Beschwer nicht entschieden werden.[12] Inzwischen wurde eine Vielzahl weiterer Eingriffsmöglichkeiten im Gesetz etabliert und umgesetzt, ohne dass zugleich grundrechtsschützende Sicherungen eingeführt wurden. Es bedarf daher einer über die obigen Vorschläge hinausgehenden **grundrechtlichen Generalüberholung des AZR** und des grundlegenden Gesetzes. Dabei sollte nicht abgewartet werden, dass der Gesetzgeber hierzu vom BVerfG verpflichtet wird.

Für Rückfragen und weitere Erläuterungen stehe ich zur Verfügung

Mit freundlichen Grüßen
Dr. Thilo Weichert

[12] BVerfG 10.10.2001 – 1 BvR 1970/95, Rn. 12, NVwZ 2002, 464.